B. AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method for preventing malicious network attacks said method comprising:

receiving a packet from a client computer;

identifying the client computer by a source IP address;

~~determining~~ calculating a number of packets received using the source IP address during a time interval; ~~and~~

comparing the number of packets received with one or more configuration settings;

determining an action from a plurality of actions based on the comparing; and

executing the action.

~~rejecting the packet in response to the number of packets exceeding a packet limit~~.

2. (Canceled)

3. (Currently Amended) The method as described in claim 1 wherein the ~~determining~~ calculating further includes:

identifying a client data area based on [[a]] the source IP address, the client data area including the number of packets received; and

incrementing the number of packets received.

4. (Canceled)

5. (Original) The method described in claim 1 further comprising:

receiving a socket request from the client computer;

determining a number of sockets opened for the client computer;

comparing the number of sockets opened to a socket limit; and

determining whether to allow a socket request based on the comparison.

6. (Canceled)

7. (Currently Amended) The method described in claim [[6]] 1 further comprising:

providing a test script, the test script including one or more attack simulations;

processing the attack simulations included in the test script;

determining whether to change one or more of the configuration settings based on the processing; and

changing one or more of the configuration settings based on the determination.

8. (Currently Amended) An information handling system comprising:

one or more processors;

a memory accessible by the processors;

one or more nonvolatile storage devices accessible by the processors;

a network interface for receiving packets from a computer network; and

~~an~~ a packet handling tool to manage packets received from the network interface, the packet handling tool including:

means for receiving a packet from a client computer through the network interface;

means for identifying the client computer by a source IP address;

means for ~~determining~~ calculating a number of packets received using the source IP address during a time interval; ~~and~~

means for comparing the number of packets received with one or more configuration settings;

means for determining an action from a plurality of actions based on the comparing; and

means for executing the action.

~~means for rejecting the packet in response to the number of packets exceeding a packet limit.~~

9. (Canceled)

10. (Currently Amended) The information handling system as described in claim 8 wherein the means for ~~determining~~ calculating further includes:

means for identifying a client data area based on [[a]] the source IP address, the client data area including the number of packets received; and

means for incrementing the number of packets received.

11. (Original) The information handling system as described in claim 8 further comprising:

means for receiving a socket request from the client computer;

means for determining a number of sockets opened for the client computer;

means for comparing the number of sockets opened to a socket limit; and

means for determining whether to allow a socket request based on the comparison.

12. (Canceled)

13. (Currently Amended) The information handling system as described in claim ~~12~~ 8 further comprising:

means for providing a test script, the test script including one or more attack simulations;

means for processing the attack simulations included in the test script;

means for determining whether to change one or more of the configuration settings based on the processing; and

means for changing one or more of the configuration settings based on the determination

14. (Currently Amended) A computer program product for preventing malicious network attacks, said computer program product comprising:

means for receiving a packet from a client computer;

means for identifying the client computer by a source IP address;

means for ~~detecting~~ calculating a number of packets received using the source IP address during a time interval; ~~and~~

means for comparing the number of packets received with one or more configuration settings;

means for determining an action from a plurality of actions based on the comparing; and

means for executing the action.

~~means for rejecting the packet in response to detecting that the number of packets exceeds a packet limit.~~

15. (Canceled)

16. (Currently Amended) The computer program product as described in claim 14 wherein the ~~determining~~ calculating further includes:

means for identifying a client data area based on [[a]] the source IP address, the client data area including the number of packets received; and

means for incrementing the number of packets received.

17. (Canceled)

18. (Original) The computer program product described in claim 14 further comprising:

means for receiving a socket request from the client computer;

means for determining a number of sockets opened for the client computer;

means for comparing the number of sockets opened to a socket limit; and

means for determining whether to allow a socket request based on the comparison.

19. (Canceled)

20. (Currently Amended) The computer program product described in claim ~~19~~ 18 further comprising:

means for providing a test script, the test script including one or more attack simulations;

means for processing the attack simulations included in the test script;

means for determining whether to change one or more of the configuration settings based on the processing; and

means for changing one or more of the configuration settings based on the determination.

21. (New) The method of claim 1 wherein the configuration settings include a first limit and a second limit, the method further comprising:

determining that the number of packets exceeds the first limit;

sending a notification in response to determining that the number of packets exceeds the first limit;

receiving a subsequent packet from the client computer;

incrementing the number of packets in response to receiving the subsequent packet;

determining that the incremented number of packets exceeds the second limit; and

rejecting the subsequent packet in response to determining that the incremented number of packets exceeds the second limit.

22. (New) The method of claim 1 wherein the configuration settings include a historical usage corresponding to the client computer, the method further comprising:
determining that the number of packets is higher than the historical usage; and
sending a notification in response to determining that the number of packets is higher than the historical usage.

23. (New) The information handling system of claim 8 wherein the configuration settings include a first limit and a second limit, the information handling system further comprising:

means for determining that the number of packets exceeds the first limit;

means for sending a notification in response to determining that the number of packets exceeds the first limit;

means for receiving a subsequent packet over the network interface from the client computer;

means for incrementing the number of packets in response to receiving the subsequent packet;

means for determining that the incremented number of packets exceeds the second limit; and

means for rejecting the subsequent packet in response to determining that the incremented number of packets exceeds the second limit.

24. (New) The information handling system of claim 8 wherein the configuration settings include a historical usage corresponding to the client computer, the information handling system further comprising:
means for determining that the number of packets is higher than the historical usage; and
means for sending a notification in response to determining that the number of packets is higher than the historical usage.

25. (New) The computer program product of claim 14 wherein the configuration settings include a first limit and a second limit, the computer program product further comprising:

means for determining that the number of packets exceeds the first limit;

means for sending a notification in response to determining that the number of packets exceeds the first limit;

means for receiving a subsequent packet from the client computer;

means for incrementing the number of packets in response to receiving the subsequent packet;

means for determining that the incremented number of packets exceeds the second limit; and

means for rejecting the subsequent packet in response to determining that the incremented number of packets exceeds the second limit.

26. (New) The computer program product of claim 14 wherein the configuration settings include a historical usage corresponding to the client computer, the computer program product further comprising:
means for determining that the number of packets is higher than the historical usage; and
means for sending a notification in response to determining that the number of packets is higher than the historical usage.